



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/550,462	04/17/2000	Pradeep Dubey	YO999-364US1	1737

30743 7590 06/21/2004

WHITHAM, CURTIS & CHRISTOFFERSON, P.C.  
11491 SUNSET HILLS ROAD  
SUITE 340  
RESTON, VA 20190

EXAMINER

KIM, JUNG W

ART UNIT PAPER NUMBER

2132

DATE MAILED: 06/21/2004

13

Please find below and/or attached an Office communication concerning this application or proceeding.

8

**Office Action Summary**

Application No.

09/550,462

Applicant(s)

DUBEY ET AL.

Examiner

Jung W Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 27 April 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 2-14 is/are allowed.
- 6) ☒ Claim(s) 1 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. Claims 1-14 have been examined. The applicant in the amendment filed on April 27, 2004 has amended claims 2 and 5.

#### ***Response to Amendment***

2. The objection to the specification is withdrawn as the amendment overcomes the objection.

#### ***Response to Arguments***

3. The following is a response to the applicant arguments listed on pages 11-17 of the amendment filed on April 27, 2004.

4. Applicant's argument, see page 12-13, with respect to the 112, 2<sup>nd</sup> paragraph rejection of claim 1 has been fully considered and is persuasive. The 112 rejection of claim 1 has been withdrawn.

5. Applicant's arguments with respect to the 103(a) rejection of claim 1 have been fully considered but they are not persuasive. Applicant argues the prior art of record does not teach receiver anonymity from the sender (see amendment, page 14, 3<sup>rd</sup> paragraph-page 16, 2<sup>nd</sup> full paragraph). However, as taught by Reiter, jondo alias is a means to mask or hide the identity of a client in a crowd (see Reiter, page 7, section 4, Crowd Overview). This technique is analogous to

Art Unit: 2132

the ubiquitous implementation of a proxy name/server for a client in which any user that connects to the client accesses the client by means of the proxy name. Hence, Reiter covers the limitation of receiver anonymity as specified in the preamble of the claim, wherein the receiver is a member of the crowd.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Reed et al. "Anonymous Connections and Onion Routing" (hereinafter Reed) in view of Reiter et al. "Crowds: Anonymity for Web Transactions" (hereinafter Reiter) and Schneier Applied Cryptography 2<sup>nd</sup> Edition (hereinafter Schneier). As per claim 1, Reed discloses a method for communication between two entities in a set of clients across a network such that no third party is able to trace the communication (see Reed, page 2, Section 2 'Onion Routing Overview') comprising the steps of:

- a. providing a set of Forwarding Agents (FAs) (see Reed, page 2, Section 2.1, 1<sup>st</sup> paragraph, 'onion proxy', 3<sup>rd</sup> paragraph);
- b. providing each of the FAs with its own pair of public and private keys for encryption and decryption, respectively, where the underlying

cryptosystem scheme is a commutative public key cryptosystem (see Reed, pages 7 and 8, Section 5.5 'Onions', 'RSA public key cryptography');

c. delivering a message through a sequence of FAs (see Reed, page 2, Section 2.1 'Operational Overview', 1<sup>st</sup> paragraph);

d. finding by the last FA in the sequence a visible network address and sending the message on to this address (see Reed, page 9, Section 5.7, 'Exit Funnel').

8. Reed is silent on the matter of each Forwarding Agent belonging to at least one group, wherein the client selects one of these groups and a message is passed randomly to a subset of FAs of this group. As taught by Reed, prior to message transmission, Onion routing initially specifies a predetermined node path to traverse from an initiator to a responder. However, transmission flows through randomly selected FAs within a defined set of FAs is a method that has been known in the art at the time the invention was made to further hide the transmission between two hosts as perceived by an unscrupulous third party. This system is called crowds and is disclosed by Reiter. Reiter teaches that crowd systems implement a group of  $n$  FAs associated with a client wherein a transmission from the client to a responder is transmitted first through a selected Forwarding Agent  $S$ , then through a randomly selected subset of the  $n$  FAs associated with the client (see Reiter, pages 7-8, Section 4, Crowd Overview). The number of FAs that are traversed by the transmission is influenced by modifying a variable of a function that determines the expected length of a

Art Unit: 2132

transmission path: this variable is the probability that a FA will forward to another FA of the group; this flexibility enables parameters to establish different types of groups in the routing methodology to match different anonymity/security requirements, (see Reiter, page 16, 3<sup>rd</sup> paragraph). Hence, by utilizing a commutative encryption algorithm (RSA is implemented for encrypting transmission information, such as destination address in the Reed invention: see Reed, page 7-8, Section 5.5 'Onions', 'RSA public key cryptography'), it would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Reiter to the invention of Reed. Motivation for such an implementation would ensure a greater degree of anonymity of the sender as taught by Reiter (see Reiter, Abstract).

9. In addition, Reiter discloses steps to anonymously register a client to a FA including adding a "jondo account name", a network address (see Reiter, page 19, 2<sup>nd</sup> paragraph), and as mentioned above, in an alternative embodiment, a group selected from a set of groups (see Reiter, page 16, 3<sup>rd</sup> paragraph, last sentence). This jondo alias conceals the sender's identity from the receiver, and the receiver's identity from the sender when the receiver is a member of the group.

10. Reed is silent on the matter of the network address being encrypted. However, sensitive data is conventionally encrypted to prevent non-authorized users from accessing the information surreptitiously. As an example, Schneier teaches means to share a secret using a threshold scheme. This type of encryption requires that a certain number of key holders are necessary to decrypt

Art Unit: 2132

the message (see Schneier, page 71, Section 3.7, 'Secret Sharing'). It would be obvious to one of ordinary skill in the art at the time the invention was made to encrypt the stored network address in the routing table of each FA using a threshold scheme to enforce anonymous transmission. Motivation for such an implementation would secure sensitive information from eavesdroppers and prevent any one individual from reading the sensitive information as taught by Schneier.

11. Finally, both Reed and Reiter are silent on the matter of each FA having keys to perform digital signatures on documents. However, as taught by Schneier in a different section, digital signatures are the standard means to verify that messages transmitted from a host is in fact transmitted from that host. Furthermore, Schneier teaches that key signatures are standard procedures to digitally signing documents (see Schneier, pages 34-44, Sections 2.6-2.7, 'Digital Signatures' and 'Digital Signatures with Encryption'). It would be obvious to one of ordinary skill in the art at the time the invention was made for each FA to have means for digitally signing transmissions. Motivation for such an implementation ensures the identity of the sender of a transmission. The aforementioned covers claim 1.

***Allowable Subject Matter***

12. Claims 2-14 are allowed.

**Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung W Kim  
Examiner  
Art Unit 2132

Jk  
June 14, 2004



GILBERTO BARRÓN  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100